Congress Races to Stay Ahead of Technology

The Bill of Rights doesn't mention cellular phones or electronic mail. But there is a growing feeling in Congress that the Fourth Amendment's guarantee against unreasonable searches was meant to protect the privacy of people using these instruments of modern technology.

Now Congress is trying to write that protection into law. In the next month the House Judiciary Committee will jump headlong into the technological era that has revolutionized communications. The challenge facing members is to develop policies that can keep pace with technology not even imagined by today's bill drafters. Industry officials say a failure to do so could cut the revolution short. Civil libertarians say it could lead to widespread abuse.

In effect, Congress is trying to practice the legislative equivalent of preventive medicine, hoping to act before a litany of problems develop. The central question is how to protect a citizen's right to privacy in the rapidly expanding communications world without unduly restricting the government's ability to monitor activities that may be illegal. *(1984 Weekly Report p. 135)*

"Congress needs to act to ensure that the new technological equivalents of telephone calls, telegrams and mail are afforded that same protection provided to conventional communications," says Robert W. Kastenmeier, D-Wis., chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and Administration of Justice, which has studied the issue.

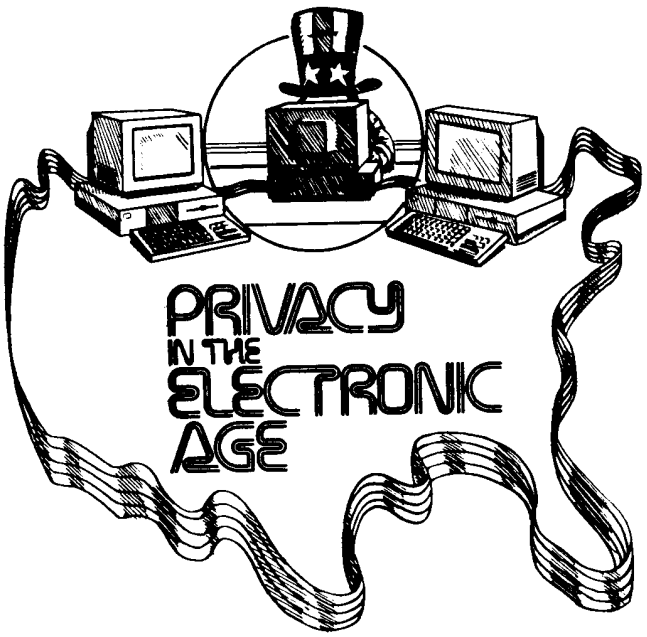
If Congress fails to act, he cautions, then "we abdicate that role to ad hoc decisions made by the courts and the executive branch."

But the courts are in no hurry to play that role, and some judges are openly asking Congress for help. In one well-circulated opinion involving video surveillance, federal Appeals Court Judge Richard Posner in Chicago said Congress needed to revise current law, adding that "judges are not authorized to amend statutes even to bring them up-to-date."

—*By Nadine Cohodas*

Keeping the Law Up With the Times

On May 14, after two years of negotiations, Kastenmeier's subcommittee approved a consensus "electronic privacy bill" (HR 3378) that members hope will be flexible enough to accommodate developing technologies.



Generally, the bill extends the privacy laws that now prohibit eavesdropping on conventional telephone and mail communications and applies them to newer forms of communications — such as mobile telephones and computer mail. *(Glossary, p. 1237)*

Law enforcement officials could intercept these high-tech communications if they obtained court orders first. Private individuals who intercept communications could face fines and prison terms.

Despite a very full congressional agenda, sponsors believe the measure has a good chance of becoming law in 1986 because of the broad coalition that is supporting it.

This coalition includes Republican and Democratic members from both chambers, the American Civil Liberties Union (ACLU), business groups that believe privacy protections are essential to continued industry growth, and the Justice Department, which did an about-face on the issue in the last year.

"I'm not going to tell you that we wiped out all opposition," says Rep. Carlos J. Moorhead, Calif., the ranking Republican on Kastenmeier's subcommittee, who helped draft the measure. "But I do think we came up with a bill that's acceptable."

Sen. Patrick J. Leahy, D-Vt., who is cosponsor of a similar Senate bill (S 1667) along with Charles McC. Mathias Jr., R-Md., is trying to get the American Bar Association (ABA) involved in the coalition. Leahy's staff is working with ABA lawyers to persuade the organization to endorse privacy legislation at its annual meeting in August.

The Senate Judiciary Subcommittee on Patents, Copyrights and Trademarks, which Mathias chairs, is expected to take up privacy legislation by the end of June.

Fourth Amendment Concerns

At the heart of the debate is the Fourth Amendment to the Constitution, which guarantees citizens protection from unreasonable searches and seizures of their property. Over the years, court cases and statutes have emerged that help define a citizen's right to privacy and the circumstances that permit government intrusions.

One of the most important laws (PL 90-351), enacted in 1968, spells out when the government may eavesdrop on voice communications carried

in part by wire over common carriers, such as the local telephone company. *(1968 Almanac p. 225)*

But even in the 1960s, members of Congress did not foresee the technological explosion that was about to occur. Within a decade of the 1968 law, concerned senators and representatives, civil liberties lawyers and private industry officials realized the law had fallen behind the technology.

The law clearly states that a standard "land-line" phone — one that operates via telephone poles, wires and underground cables — cannot be tapped at random. But what about a phone that works by radio waves? And what about "electronic mail," where individuals have conversations by computer?

These questions germinated through the late 1970s and into the 1980s. Congressional efforts began to take shape throughout 1984, when Kastenmeier held a series of hearings on civil liberties and "the national security state."

The hearings, which were timed specifically to coincide with the year of George Orwell's futuristic, political novel "1984," helped focus attention on new forms of technology and how to reconcile technology with privacy protections and law enforcement concerns.

"We sort of got beyond ideological labels and talked about principles," said one congressional aide. "Witnesses identified gaps in the law."

Building a Coalition

The ACLU sought to build on the Kastenmeier hearings, and Jerry Berman, the ACLU's chief legislative counsel, put together two conferences on privacy and technology in June 1984 and January 1985. Participants included civil liberties lawyers, industry representatives, executive branch officials and congressional staff.

"We saw the consultation as an opportunity to explore the possibility of a political coalition," Berman says. "The ACLU approached this from the view that the content of private messages ought to be protected under law regardless of the means of communication."

Although the ACLU had worked on privacy issues for years, Berman says he realized legislation "would never get off the ground until we got a new coalition. As long as privacy groups were just talking to each other, nothing was going to happen. We thought business could be convinced [to get involved] if we could show them it was in their own economic self-interest."

Business involvement was also important politically in getting the Justice Department interested. "Particularly in this administration, if the ACLU were in the lead, this bill would go nowhere," Berman says. Indeed, when he was counselor to the president, Attorney General Edwin Meese III once disparaged the ACLU as the "criminals' lobby."

Another important factor was a report — "Electronic Surveillance and Civil Liberties"— published in October 1985 by the Office of Technology Assessment (OTA), an arm of Congress whose main function is to help members anticipate and plan for the effects of technological change.

The report provided some hard data, according to one congressional aide, about surveillance techniques available through new technology. It also provided data on which government agencies already used new methods, which agencies had plans to upgrade their tracking systems and the extent of government surveillance already occurring.

For example, the report noted that the number of court-approved bugs and wiretaps in 1984 was the highest ever — 801. More than half of the court orders, 512, were by state judges, and the remaining 289 were by federal judges. Only one request for a court order was rejected.

In addition, about 25 percent of the federal agencies responding to an OTA survey said they either used or planned to use various electronic surveillance technologies, including closed-circuit television, electronic beepers and sensors, computer and electronic-mail monitoring devices, and devices for intercepting "cellular" phones.

Conversations on these phones are transmitted by high-frequency radio signals to a base station, which in turn connects the calls to an existing conventional land-line phone system or to another base station.

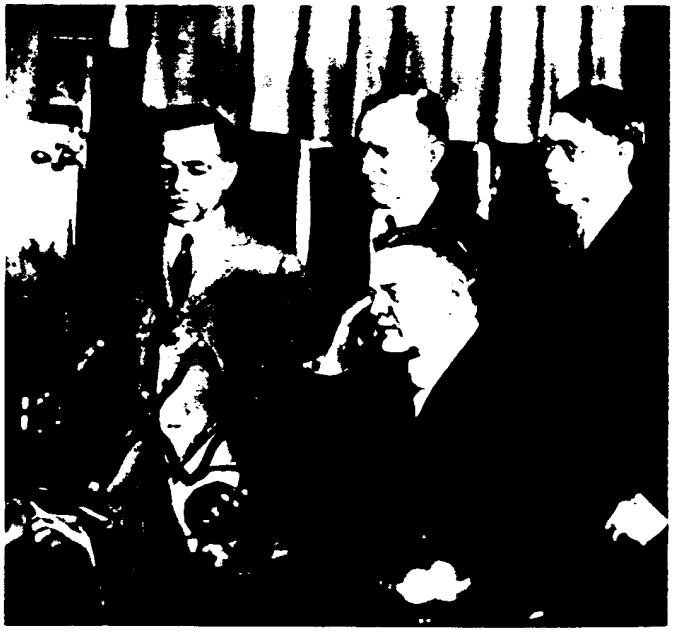
The OTA report also noted that the agencies responding reported a total of 85 computerized systems with, collectively, about 288 million records on 114 million people.

While the report offered policy "options" rather than specific recommendations, it asserted that "the existing statutory framework and judicial interpretations thereof do not adequately cover new and emerging technologies."

As a result, the report said, the government, by its use of new electronic surveillance techniques, could infringe on individuals' constitutional rights.

The OTA report and the ACLU conferences helped convince electronics industry officials that they had much to gain and little to lose by new legislation.

Judiciary Subcommittee Chairman Robert W. Kastenmeier, D-Wis., left, drafted the original electronic-privacy bill, but it was ranking minority member Carlos J. Moorhead, R-Calif., who helped make the bill acceptable to the Justice Department. "I'm not going to tell you that we wiped out all opposition," said Moorhead, "but I do think we came up with a bill that's acceptable."



Privacy laws have been outdated by the growth in communications technology. A mobile telephone that uses radio waves to transmit signals does not receive the same protection today as does the standard telephone that sends its message by wire. At right, Herbert Hoover demonstrates the best telephone technology available in 1927, when Hoover was secretary of commerce.

Unlike the 1968 wiretap law, which was enacted in response to abuses in government eavesdropping, the privacy coalition hopes to get legislation enacted that provides a solution before there is a problem.

"Given the fact that more and more Americans are using electronic messaging technology, laying the ground rules now will prevent problems in the future," says Michael F. Cavanagh, executive director of the Electronic Mail Association, which represents 80 communications service and electronic equipment companies.

"It would be better for the industry to pass this bill," he adds, referring to HR 3378.

A similar view comes from Barbara Phillips of Telocator Network of America, a trade association for companies that provide two-way radio and paging services to the public along with cellular phones.

"The users of our communications systems anticipate and very much want privacy for their communications," she says, "and by clarifying the law, it's good public policy for Congress and good consumer policy for us."

In testimony last November before the Senate Patents Subcommittee, John Stanton, chairman of Telocator, warned members that new legislation was necessary to foster growth in the industry. Failure to enact new privacy protections, Stanton asserted, would discourage the use of many new communications devices, "thereby stifling emerging industries and limiting the benefits" to the public.

Convincing Justice

Getting the Justice Department to go along was another matter. In September 1984 Justice officials indicated at separate House and Senate hearings that the basic 1968 wiretap law did not need any change.

Testifying Sept. 12, 1984, before the Senate Judiciary Patents Subcommittee, John Keeney, of the department's criminal division, said there was a "reluctance to tinker" with the law and that Justice officials would be "very sensitive to any amendments that would lessen our ability to use what we consider to be a very effective tool."

Two weeks later, in testimony before Kastenmeier's House subcommittee, Mary Lawton, the director of the Office of Intelligence Policy and Review, said she could not say there was any consensus for change within the department. But she said she believed the 1968 law needed clarification.

Kastenmeier already had drafted a bill, and after he introduced the measure, he sent it to the department as well as to industry and civil liberties lawyers for comment. In May 1985 Lawton sent a letter to Kastenmeier with several criticisms of the bill and recommendations for action, triggering a long round of negotiations with Justice officials.

The department's chief concerns were over the circumstances and procedures that would allow government eavesdropping. Officials wanted to make sure that the department's ability to tap or bug phones and computers was not unduly restricted. Industry representatives and civil libertarians, on the other hand, wanted to make sure that electronic communications could be kept private except in very limited cases.

Moorhead, who often represents the department's views on legislation in the committee, was an important part of the process. When it appeared that Justice was reluctant to participate in talks on the legislation, he urged officials to keep meeting with industry representatives and congressional staffers.

As a result of the extensive talks, Kastenmeier and the subcommittee deleted a number of provisions from the original bill that had drawn Justice Department objections. Most of these involved changes in procedures for getting court-ordered wiretaps and bugs.

But even with these changes, Justice was still not firmly behind the bill, and without its support, which

was crucial in getting wider administration backing. Kastenmeier was reluctant to press ahead.

A key date in the negotiations was last April 29, when Alexander B. Trowbridge, president of the National Association of Manufacturers, wrote Attorney General Meese telling him how important the Kastenmeier bill was to industry.

In the "Dear Ed" letter, Trowbridge urged Meese to give his "personal attention" to helping resolve the differences holding up the agreement.

When the subcommittee took up the bill two weeks later, Justice, industry, civil liberties lawyers and congressional drafters finally had reached a consensus.

"All of these things built up," said one House aide, citing the department's turnaround. "You had the ranking minority telling them, 'We have to have this. Meet with industry.' And industry saying, 'We need this. There are no rules here.' "

Justice did force some changes in the bill that will "make their life easier," a staffer said. A major revision is a new section that will allow the department to get "roving" telephone taps to follow suspects who are deliberately trying to avoid surveillance by using pay phones.

Instead of having to request a tap on a specific telephone, the department could get permission to tap any phone while the suspect was using it, as long as a judge is convinced that an investigation would otherwise be thwarted.

The ACLU's Berman said these and some other procedural changes are reasonable and acceptable.

How the Bill Works

The basic idea of HR 3378 is to protect communications between individuals regardless of the means of transmission. The bill rewrites the 1968 wiretap law to protect "electronic communications" — a newly defined term covering "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature" that is transmitted "in whole or in part by wire, radio, electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce."

However, the bill would not protect any radio communication that is "readily accessible" to the general public. A radio signal would be protected from intrusion in several specific instances: if the signal were scrambled or put into code, that is, "encrypted"; if the signal's frequency were changed to one withheld from general use by the Federal Communications Commission (FCC); if the signal were transmitted through a "common carrier," like a cellular-telephone company that serves the public; or if the signal were transmitted via specific radio frequencies set out in the bill.

These definitions mean that cordless telephones, which operate through low-frequency radio waves, would not be covered. Low frequencies are easily intercepted, often by accident. The subcommittee reasoned that owners of such phones have a lesser expectation of privacy than owners of more conventional phones, and should therefore not be protected from interception.

A Kastenmeier memo to his subcommittee noted that cordless-phone owners can ensure privacy by obtaining inexpensive devices that will transform conversations into code while they are being transferred. The memo also noted that the FCC has required only that a cordless phone include a disclaimer explaining that users cannot be assured of privacy during their calls.

Private Interception. The bill makes it illegal for individuals to intercept electronic communications as defined in the bill. The offense is a felony, and the penalty with some exceptions is a fine, a prison term of up to five years, or both.

The exceptions include interception of radio communications (other than the radio portion of a cellular phone call), for which the maximum prison term is one year.

If the interception is the radio portion of a cellular call, the violation in most instances is only a petty offense, and the penalty is a fine of up to $500 and a maximum prison term of six months, or both.

These provisions for radio interception are premised on the argument that such intrusions are easier to make and require less intent on the part of the violator. Hence, this reasoning continues, the penalties should be lighter than for other kinds of interceptions, which require a higher degree of sophistication and a correspondingly higher level of intent to violate the law.

The bill also makes it illegal for a person or entity providing wire or electronic communication service to the public to divulge knowingly the contents of any communication except to the person sending the information or the intended recipient.

The American Civil Liberties Union played a major role in bringing business into a coalition supporting a new privacy law. ACLU counsel Jerry Berman says he realized "as long as privacy groups were just talking to each other, nothing was going to happen."

Government Interception. HR 3378 allows the government to intercept "electronic communications" after officials have obtained a court order. A judge can grant the order after he has determined that the interception "may provide or has provided evidence of any federal felony."

The bill also includes a provision allowing law enforcement officials to get court approval for a "mobile tracking device" that goes beyond the geographic jurisdiction of the court. The only proviso is that the device — which is used to track a moving suspect — be installed in the jurisdiction of the judge who approved the order.

(Federal courts are divided by geographic region within the 50 states and selected federal territories.)

Stored Communications. The bill includes a separate section covering stored communications, an essen-